DETAILED ACTION

1. This is in response to the arguments filed on 07/15/2008.

2. Claims 1, 4-24 are pending in the application.

3. Claims 1, 4-24 have been rejected.

Response to Amendment

4. The examiner approves the amendments made to claims 1, 17, and 22.

5. The examiner withdraws the 112 first and second paragraphs rejections as necessary amendment and explanation have been made.

Response to Arguments

6. Applicant's arguments with respect to claims 1, 4-24 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 4-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baggett et al hereafter Baggett (US patent 6,925,443) in view of Alling (US Patent Publication 20020194329).

8. As per claim 1, Baggett discloses a method comprising: collecting security information from the computers of the first enterprise under audit; analyzing the security information and providing a first result of this analysis (col. 3, lines 52-67, col. 6, lines 24-39, col. 22, lines 9-30); and comparing this first result with a second result comprising information derived from information previously obtained through application of the collecting and analyzing steps, the result of this comparing step indicating the relative security of the first enterprise under audit (col. 7, lines 5-15, col. 12, lines 25-40, lines 55-63, col. 16, lines 25-45, col. 17, lines 1-15, col. 18, lines 12-42, col. 19, lines 35-67, col. 20, lines 1-5), where a peer group is defined to be a group of one or more enterprises assigned to the same business category as the first enterprise, enterprises involved in the same (or a similar) industry or business as the first enterprise, enterprises having computers configured similarly to the first enterprise's computers, or enterprises required to comply with the same security standards as the first enterprise, or a combination of these (col. 3, lines 20-32, lines 52-67, col. 6, lines 24-39, col. 8, lines 19-27, col. 22, lines 9-30). Although, Baggett discloses comparing the stored security measures with the audited security measures of enterprise. He does not expressly disclose that comparing the results with the one or more peer groups enterprises. However, in the same field of endeavor, Alling discloses comparing this first result with a second result comprising information derived from information previously

obtained through application of the collecting and analyzing steps to one or more other enterprises that interconnect the computing environments of other different organizations of people, these one or more other enterprises together forming a relevant peer group of other different organizations of people (paragraphs, 0016-0017), where a peer group is defined to be a group of one or more enterprises assigned to the same business category as the first enterprise, enterprises involved in the same (or a similar) industry or business as the first enterprise, enterprises having computers configured similarly to the first enterprise's computers, or enterprises required to comply with the same security standards as the first enterprise, or a combination of these (paragraphs, 0013-0015).

Accordingly, it would been obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Alling's teachings of comparing the audited results with the other peer groups enterprises combined with the teachings of Baggett, for the purpose of suitably measuring the audited enterprise security status with peer group security standards.

9. As per claim 4, Baggett discloses the method comprising the step of generating at least one report that presents the first and second results arranged in a way that facilitates their comparison (col. 16, lines 25-45, col. 17, lines 1-15, col. 18, lines 12-42, col. 19, lines 35-67, col. 20, lines 1-5).

10. As per claim 5, Baggett discloses the method wherein the generating step includes presenting the first and second results each broken down into several results relating to several different areas of security, with a first and a second result presented

for each different area of security and arranged in a way that facilitates their comparison (col. 7, lines 5-15, col. 12, lines 25-40, lines 55-63, col. 16, lines 25-45, col. 17, lines 1-15, col. 18, lines 12-42).

11. As per claim 6, Baggett discloses the method wherein in the generating step, the results relating to several different areas of security comprise results arising from analysis of personnel security information and physical security information, at least some of the information included in the first result having been gathered using interviews during the collecting step (col. 16, lines 25-45, col. 17, lines 1-15, col. 18, lines 12-42, col. 19, lines 35-67, col. 20, lines 1-5).

12. As per claim 7, Baggett discloses the method wherein, in the generating step, the results relating to several different areas of security comprise results arising from analysis of password security information and file access permission security information (col. 17, lines 1-15, col. 18, lines 12-42, col. 19, lines 35-67, col. 20, lines 1-5).

13. As per claim 8, Baggett discloses the method wherein, in the generating step, the results relating to several different areas of security further comprise results arising from analysis of personnel security information and physical security information, at least some of the information included in the first result having been gathered using interviews during the collecting step (col. 17, lines 4-15, col. 18, lines 12-42, col. 19, lines 35-67, col. 20, lines 1-5).

14. As per claim 9, Baggett discloses the method wherein, in the generating step, the several different areas of security comprise one or more results of analysis of computer

configuration security information and one or more results of analysis of security information gathered using interviews (col. 7, lines 5-15, col. 12, lines 25-40, lines 55-63, col. 16, lines 25-45, col. 17, lines 1-15, col. 18, lines 12-42).

15. As per claim 10, Baggett discloses the method wherein, in the generating step, the one or more results of analysis of computer configuration security information comprise results arising from analysis of password security information (col. 16, lines 25-45, col. 17, lines 1-15, col. 18, lines 12-42, col. 19, lines 35-67, col. 20, lines 1-5).

16. As per claim 11, Baggett discloses the method wherein, in the generating step, the one or more results of analysis of computer configuration security information comprises results arising from analysis of file access permission security information (col. 17, lines 1-15, col. 18, lines 12-42, col. 19, lines 35-67, col. 20, lines 1-5).

17. As per claim 12, Baggett discloses the method wherein the generating step generates at least two comparative reports in different formats for different requesting parties or uses, and in particular one for technical experts that includes technical language and details and another for non-technical-experts that substantially excludes technical language and details (col. 12, lines 25-40, lines 55-63, col. 16, lines 25-45, col. 17, lines 1-15, col. 18, lines 12-42).

18. As per claim 13, Baggett discloses the method wherein generating and executing commands to alter the security information of one or more computers to improve system security in at least some cases when the analysis or comparison or both indicate security is in need of improvement (col. 7, lines 5-15, col. 12, lines 25-40, lines 55-63, col. 16, lines 25-45, col. 17, lines 1-15, col. 18, lines 12-42).

19. As per claim 14, Baggett discloses the method wherein generating at least one report that presents the first and second results arranged in a way that facilitates their comparison (col. 16, lines 25-45, col. 17, lines 1-15, col. 18, lines 12-42, col. 19, lines 35-67, col. 20, lines 1-5).

20. As per claim 15, Baggett discloses the method wherein the generating commands step generates commands which force the deactivation or correction of one or more passwords when the analysis or comparison or both indicate that these one or more passwords are not sufficiently secure (col. 17, lines 1-15, col. 18, lines 12-42, col. 19, lines 35-67, col. 20, lines 1-5).

21. As per claim 16, Baggett discloses the method wherein the generating commands step generates commands which force alteration of one or more configuration file or control file access permissions if the analysis or comparison or both indicate that the access permissions assigned to these one or more files do not provide adequate system security (col. 12, lines 25-40, lines 55-63, col. 16, lines 25-45, col. 17, lines 1-15, col. 18, lines 12-42).

22. As per claim 17, Baggett discloses a system comprising: a plurality of computers within the first enterprise under audit; collectors associated with the computers and arranged to collect from the computers information concerning the security of the first enterprise under audit; a security analyzer arranged to analyze the information concerning the security of the first enterprise under audit and to provide a first result of this analysis (col. 3, lines 52-67, col. 6, lines 24-39, col. 22, lines 9-30); a data base containing a second result comprising information derived from information previously

obtained through application of the collectors and security analyzer, a comparison mechanism arranged to compare the first and second results to determine the relative security of the first enterprise under audit (col. 7, lines 5-15, col. 12, lines 25-40, lines 55-63, col. 16, lines 25-45, col. 17, lines 1-15, col. 18, lines 12-42, col. 19, lines 35-67, col. 20, lines 1-5), where a peer group is defined to be a group of one or more enterprises assigned to the same business category as the first enterprise, enterprises involved in the same (or a similar) industry or business as the first enterprise, enterprises having computers configured similarly to the first enterprise's computers, or enterprises required to comply with the same security standards as the first enterprise, or a combination of these (col. 3, lines 20-32, lines 52-67, col. 6, lines 24-39, col. 8, lines 19-27, col. 22, lines 9-30). Although, Baggett discloses comparing the stored security measures with the audited security measures of enterprise. He does not expressly disclose that comparing the results with the one or more peer groups enterprises. However, in the same field of endeavor, Alling discloses a data base containing a second result comprising information derived from information previously obtained through application of the collectors and security analyzer to one or more other enterprises that interconnect the computing environments of other different organizations of people these one or more other enterprises together forming a relevant peer group of other different organizations of people (paragraphs, 0016-0017); where a peer group is defined to be a group of one or more enterprises assigned to the same business category as the first enterprise, enterprises involved in the same (or a similar) industry or business as the first enterprise, enterprises having computers configured

similarly to the first enterprise's computers, or enterprises required to comply with the same security standards as the first enterprise, or a combination of these (paragraphs, 0013-0015).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 17.

23. Claims 18-21 are listed all the same elements of claim 5-16 but in system form rather than method form. Therefore, the supporting rationales of the rejection to claim 5-16 apply equally as well to claim 18-21.

24. As per claim 22, Baggett discloses a system comprising: a plurality of computers within the first enterprise under audit; collectors associated with the computers and arranged to collect from the computers information concerning the security of the first enterprise under audit; a security analyzer arranged to analyze the information concerning the security of the first enterprise under audit and to provide a first result of this analysis (col. 3, lines 52-67, col. 6, lines 24-39, col. 22, lines 9-30); a data base containing a second result comprising information derived from information previously obtained through application of the collectors and security analyzer, a comparison mechanism arranged to compare the first and second results to determine the relative security of the first enterprise under audit (col. 7, lines 5-15, col. 12, lines 25-40, lines 55-63, col. 16, lines 25-45, col. 17, lines 1-15, col. 18, lines 12-42, col. 19, lines 35-67, col. 20, lines 1-5), where a peer group is defined to be a group of one or more enterprises assigned to the same business category as the first enterprise, enterprises involved in the same (or a similar) industry or business as the first enterprise,

enterprises having computers configured similarly to the first enterprise's computers, or enterprises required to comply with the same security standards as the first enterprise, or a combination of these (col. 3, lines 20-32, lines 52-67, col. 6, lines 24-39, col. 8, lines 19-27, col. 22, lines 9-30). Although, Baggett discloses comparing the stored security measures with the audited security measures of enterprise. He does not expressly disclose that comparing the results with the one or more peer groups enterprises. However, in the same field of endeavor, Alling discloses a data base containing a second result comprising information derived from information previously obtained through application of the collectors and security analyzer to one or more other enterprises that interconnect the computing environments of other different organizations of people these one or more other enterprises together forming a relevant peer group of other different organizations of people (paragraphs, 0016-0017); where a peer group is defined to be a group of one or more enterprises assigned to the same business category as the first enterprise, enterprises involved in the same (or a similar) industry or business as the first enterprise, enterprises having computers configured similarly to the first enterprise's computers, or enterprises required to comply with the same security standards as the first enterprise, or a combination of these (paragraphs, 0013-0015).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 22.

25. Claims 23-24 are listed all the same elements of claim 5-16 but in system form rather than method form. Therefore, the supporting rationales of the rejection to claim 5-16 apply equally as well to claim 23-24.

Conclusion

26. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **MOAZZAMI NASSER G** can be reached on **(571)272-4195**. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Nasser G Moazzami/ /Mohammad W Reza/

Supervisory Patent Examiner, Art Unit 2436 Examiner, Art Unit 2436